Passkeys - anmelden ohne Passwort

Was sind Passkeys?

Passkeys sind ein moderner Anmeldestandard, mit dem man sich bei Webseiten und Apps ohne klassisches Passwort anmelden kann. Statt eines Passworts wird beim Login lediglich der Fingerabdruck, ein Gesichtsscan oder die Geräte-PIN abgefragt, um die eigene Identität zu bestätigen. Technisch basiert das Ganze auf dem offenen FIDO2/WebAuthn-Standard, den neben Apple, Google und Microsoft auch Unternehmen wie Amazon, PayPal, eBay, GitHub und viele weitere unterstützen.

Wie funktionieren Passkeys?

Bei der Einrichtung eines Passkeys wird ein **Schlüsselpaar** erzeugt: ein privater Schlüssel, der Ihr Gerät oder Ihren Sicherheitsschlüssel niemals verlässt, und ein öffentlicher Schlüssel, der beim jeweiligen Onlinedienst hinterlegt wird. Da niemand mehr ein Passwort eintippen oder speichern muss, gibt es auch nichts mehr, das gestohlen, erraten oder bei einem Datenleck kompromittiert werden könnte.

Unterschiede zwischen Passwort und Passkey

Passkeys eliminieren mehrere der größten Schwachstellen klassischer Passwörter auf einen Schlag:

- Kein Phishing mehr möglich, da der private Schlüssel niemals an den Dienst übertragen wird und nur zur passenden Webadresse funktioniert
- Kein Wiederverwenden schwacher oder mehrfach genutzter Passwörter, da für jeden Dienst automatisch ein einzigartiges Schlüsselpaar erzeugt wird
- Selbst wenn ein Onlinedienst gehackt wird, können Angreifer aus dem öffentlichen Schlüssel keinen Login-Zugriff ableiten

Wichtig zu wissen: Solange ein Dienst weiterhin die klassische Passwort-Anmeldung parallel anbietet, bleibt das Konto über dieses Passwort weiterhin angreifbar. Der volle Sicherheitsgewinn entsteht erst, wenn das Passwort für den jeweiligen Account vollständig deaktiviert wird.

Einrichtung eines Passkeys im Enpass Passwortmanager

https://www.youtube-nocookie.com/embed/JDfx9L4BS60?si=w_VAKFZwQSQG4Ysy

Anleitung folgt

Einrichtung eines Passkeys auf dem Sicherheitsschlüssel

Anleitung folgt

Was man bei der Verwaltung und Nutzung von Passkeys unbedingt berücksichtigen muss

Auf den ersten Blick ist es bequem, Passkeys direkt im iCloud-Schlüsselbund, im Google Passwortmanager oder im Microsoft-Konto zu speichern – schließlich bieten alle drei Konzerne diese Option standardmäßig an.

Aus Sicherheits- und Unabhängigkeitsgründen raten wir davon jedoch ausdrücklich ab, und zwar aus folgenden Gründen:

- **Bindung an das Ökosystem (Vendor Lock-in)**: Apple, Google und Microsoft implementieren Passkeys so, dass Nutzer stark an das jeweilige Ökosystem gebunden werden. Ein bei Apple erstellter Passkey lässt sich zwar automatisch zwischen Apple-Geräten synchronisieren, funktioniert aber auf einem Windows-PC oder Android-Gerät nur mit Umwegen wie einem QR-Code-Login über das iPhone.
- **Keine echte Exportmöglichkeit**: Ein zentrales Problem ist, dass Apple und Google den Export gespeicherter Passkeys nicht erlauben. Wer zu einem anderen Anbieter wechseln möchte, muss sämtliche Passkeys komplett neu erstellen. Das ist vergleichbar damit, dass man nicht einmal eine Kopie des eigenen Wohnungsschlüssels anfertigen dürfte.
- **Abhängigkeit vom eigenen Konto**: Bei Apple ist der private Schlüssel in der Cloud an die Apple-ID gekoppelt – ohne aktive Apple-ID gibt es keine Wiederherstellung. Bei Google ist der Zugriff an das Google-Konto gebunden, bei Microsoft an das Microsoft-Konto. Wird das jeweilige Konto gesperrt, kompromittiert oder aus anderen Gründen unzugänglich, verliert man potenziell den Zugriff auf alle darin gespeicherten Passkeys.
- **Wirtschaftliche Interessen statt Interoperabilität**: Kritiker weisen darauf hin, dass die großen Tech-Konzerne Passkeys gezielt nutzen, um Kunden noch enger an ihre eigenen Dienste zu binden, statt konsequent auf plattformübergreifende Nutzbarkeit zu setzen.

Version #5
Erstellt: 2026-07-25 13:11:02 UTC von Marvin Meißner
Zuletzt aktualisiert: 2026-07-25 13:22:17 UTC von Marvin Meißner